No.59
November 2022

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ SPONSORED**

Streamlining Telco SOC Operations

Sponsored by NetQuest Corporation

- NetQuest's Network Security Broker is a new Traffic Policy Engine for telco security operations. It provides granular SOC grey-listing and other DPI-based traffic classification at the service provider edge at line rate at 100 and 400 Gbit/s.
- Traffic continues to show high growth rates but most of it is going dark and most of it is traffic security operations doesn't need eyes on. By stripping out the majority of traffic that the SOC does not need to see, a Network Security Broker can streamline SOC operations to drive high security efficacy with better cost efficiency.

What a time this is to be running telco security operations. For the year ending 2021, Orange Group reports that its data traffic in Europe increased by 33% on 2020. In May 2022, Vodafone CTO, Johan Wibergh, said data consumption is growing at around 40% a year. Migration from 4G to 5G, and from 10 Gbit/s to 100 Gbit/s - ultimately 200 Gbit/s and 400 Gbit/s - optical systems are key drivers and enablers of this growth.

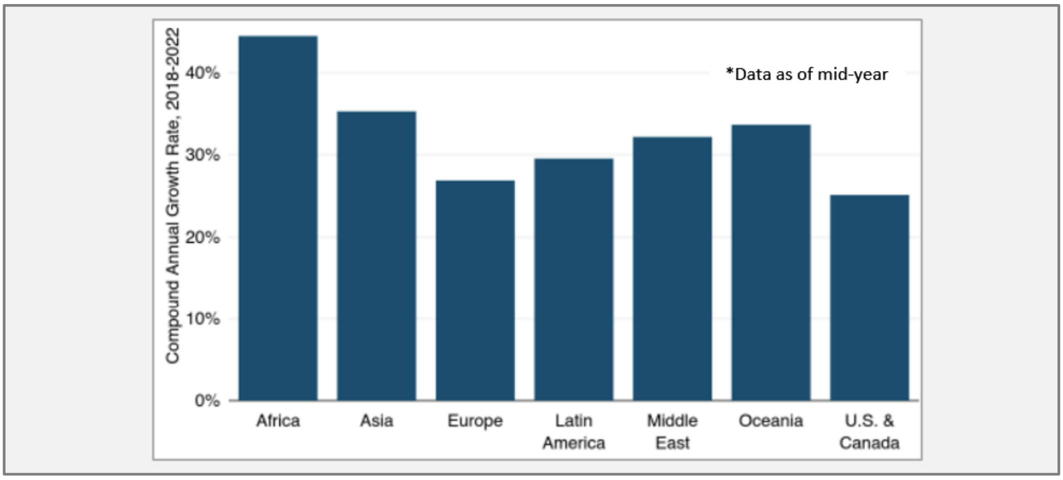
There's near-universal agreement that 70% or more of network traffic is encrypted now.

That growth comprises a lot more good traffic, most of which is video (the bulk of which a telco's Security Operations Centre or SOC does not need to see). But there's growth in malicious traffic too. And with 5G, some security monitoring requirements will need pushing out to the service provider edge. Whereas most businesses don't have much to fear from advanced nation state cyber threats in the malicious traffic they see, telcos are among their primary targets. Also, whereas most organizations depend on the network to maintain their business operations, telcos provide the network that enables hundreds of thousands, if not millions, of users to stay online. Telcos are the network.

Telco SOC Operations Teams Face Strong Headwinds

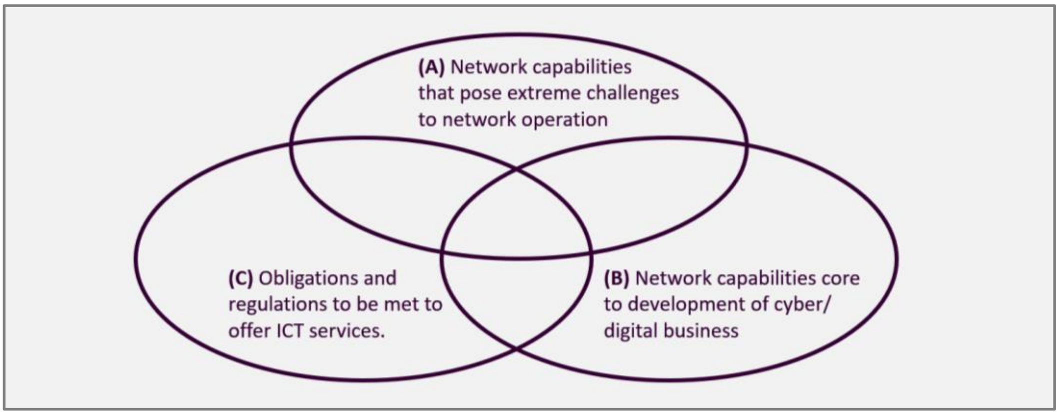
These are already strong headwinds for a telco SOC to be contending with but there are still more. Fortinet points to 2017 as the year when the share of all web traffic that is encrypted surpassed 50%. Nokia reckons that happened in February 2019. Either way, there's near-universal agreement that 70% or more of network traffic is encrypted now.

Figure 1: International Internet Bandwidth Growth by Region



Source: Telegeography, September 2022, http://www2.telegeography.com

Figure 2: Encryption of Services is Causing Networks to 'Go Dark'


(A) Network capabilities that pose extreme challenges to network operation
(C) Obligations and regulations to be met to offer ICT services.
(B) Network capabilities core to development of cyber/ digital business

Source: ETSI, "Encrypted Traffic Integration (ETI): Problem Statement", June 2021

As well as providing additional security protection, encryption of traffic on this scale has also introduced substantial new security risk. That's because while encryption gets used to protect legitimate traffic, cyber threat actors have also become adept at exploiting encryption to protect their malicious code against detection by security controls.

ETSI has defined a challenge of 'Encrypted Traffic Integration' (ETI)

The telecom sector's challenge as regards "Encrypted Traffic Integration" is defined by ETSI as shown in **Figure 2**. It consists of maintaining, if not improving, network security as required by customers and regulators (C) while faced with the risk of the efficacy of conventional network threat detection controls being evaded by network-level encryption by networks and applications (A) as well as additional layers of encryption applied by end users themselves (B).

TLS 1.3, which accounts for most transport layer encryption now, enables perfect forward secrecy by default.

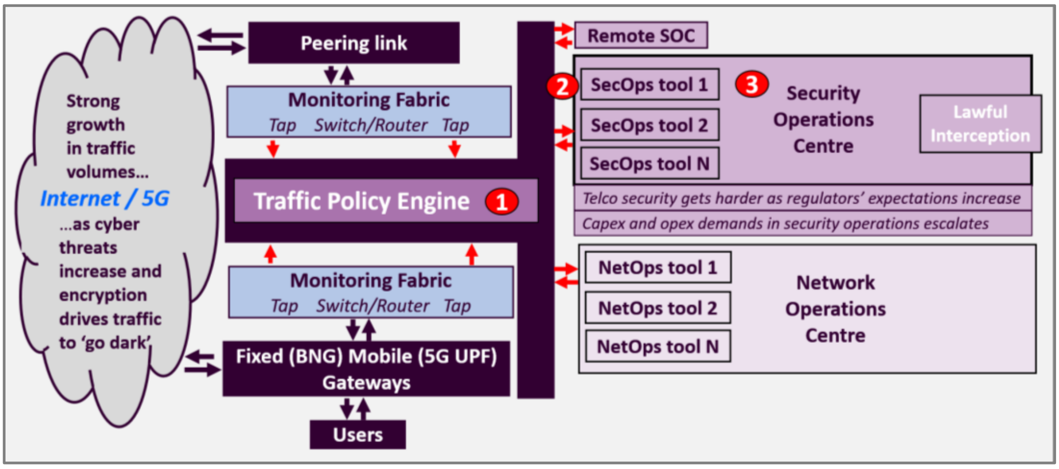
It's not just encryption per se that has created new challenges for security operations, it's the particular type of encryption. TLS 1.3, which accounts for most transport layer encryption now, enables perfect forward secrecy by default. The encryption keys are purposely ephemeral and constantly changing so that only the two endpoints can decrypt the traffic. Hence the traditional option for authorized users like telcos to access encryption keys and decrypt traffic for security monitoring no longer works. Most traffic has therefore largely "gone dark" to the telco SOC. In its June 2021 report "Encrypted Traffic Report; Problem Statement" ETSI defines this as "phenomena by which an authorized user lacks the technical or practical ability to access data."

HTTP3 is used by 25% of websites – making traffic go darker still

This problem will be compounded at the application layer by the IETF's adoption of HTTP3 as a standard in June 2022. HTTP3 replaces Transmission Control Protocol (TCP) used in HTTP and HTTP2 with Google's 'QUIC' protocol and User Datagram Protocol (UDP). Internet giants like Google and CDN providers like Cloudflare and Akamai are ardent supporters of HTTP3 because it enables faster web browsing speeds and lower latency. As of August 2022, W3techs.com shows 25% of websites are already using it. From a security operations perspective, however, HTTP3 makes traffic go darker still. That's because it takes some of the transport-specific information that TCP left unencrypted and encrypts it by default.

In other circumstances, a regulated business facing such pressures might expect some regulatory relief. In fact, rather than lowering them, most governments are ratcheting up their expectations of telcos when it comes to cyber security. The UK's new Telecommunications Security Act, that came into effect a year ago, is just one of many examples of higher government expectations on telcos coupled with stiffer penalties. Telcos can be fined up to 10% of revenues for non-compliance with the UK's new law.

Figure 3: A High Level Telco Security Operations Architecture


Strong growth in traffic volumes...
Internet / 5G
...as cyber threats increase and encryption drives traffic to 'go dark'
Peering link
Monitoring Fabric
Tap Switch/Router Tap
Traffic Policy Engine
1
Monitoring Fabric
Tap Switch/Router Tap
Fixed (BNG) Mobile (5G UPF) Gateways
Users
Remote SOC
2
SecOps tool 1
SecOps tool 2
SecOps tool N
3
Security Operations Centre
Lawful Interception
Telco security gets harder as regulators' expectations increase
Capex and opex demands in security operations escalates
NetOps tool 1
NetOps tool 2
NetOps tool N
Network Operations Centre

Source: HardenStance

As well as finding solutions to the challenges that 'going dark' poses to their own business operations, governments also expect telcos to help find solutions to the challenges that it presents to law enforcement in carrying out lawful interception. In summary, there's both more good and more bad traffic hitting the network and it's increasingly difficult to distinguish one from the other. And if anything, the imperative of a telco's security operations team making the right calls is greater than ever.

A monitoring 'fabric' can be based on Network Packet Brokers or lower cost L2/L3 switches that aggregate all the traffic the SOC wants to see.

The Role of the Monitoring Function in SOC Operations

This Briefing takes a look at today's telco security operations model. From left to right, **Figure 3** depicts traffic coming into the telco network via its mobile and fixed network gateways as well as via peering links. Security operations needs to view some of that traffic either in line or out of band using network taps, span ports or splitters. The term 'Monitoring Fabric' is used here to describe their own implementations by advanced telco SOC organizations.

The primary functions performed here in an engineered monitoring fabric are:

- **Aggregation** – forwarding of one single stream of data to relevant security tools.
- **Replication** – forwarding copies of the same data to the SOC for parallel analysis.
- **Load balancing** – ensuring no one instance of a security tool gets overloaded.

This 'fabric' can be based on Network Packet Brokers or lower cost L2/L3 switches that aggregate all the traffic the SOC wants to see. Telcos that don't have a universal monitoring fabric tend to feed network taps directly into local switches or Network Packet Brokers to feed traffic to SOC tools.

High Security Efficacy and Cost Efficiency are Equally Important

The focus of this Briefing is (1) the Traffic Policy Engine in **Figure 3** where traffic inspection, classification and optimization take place. What matters in terms of both security efficacy and cost is that each and every flow or packet that does need to be forwarded on to a specific security tool should indeed be forwarded.

In the case of some critical services, or perhaps traffic originating or terminating in a specific country, a SOC needs to get eyes on every single flow and every single packet, down to every last byte. Just as importantly, though, any traffic that doesn't need to be forwarded to a security tool should not be. Instead it should either be dropped or returned to the production network.

In the context of SOC monitoring, classification and optimization, the terms ‘blacklisting’ and ‘whitelisting’ have a slightly different meaning than the usual one. SOC blacklisting is for traffic that the SOC doesn’t need to see at all. Hence that good traffic actually needs to be blacklisted – i.e, blocked from being forwarded to the SOC where it would only consume resources unnecessarily. SOC whitelisting is for traffic that the SOC wants to see all of. Hence it requires whitelisting – forwarding to the SOC in its entirety. 5G control plane traffic is a good example of traffic a SOC would typically want to whitelist.

The accuracy with which only the right packets are forwarded to the SOC is key to keeping the lid on capex and opex costs. The techniques available to a traffic optimization engine to drive the best possible inspection, classification and optimization outcomes are characterized below:

- **Packet filtering** – discriminating between packets based on source destination addresses, ports and protocols to remove data the SOC doesn’t need or discriminate between those applications that pose a risk and those that don’t.
- **Packet Inspection** – discriminating between packets based on specific payloads or other data.
- **Packet Optimization** – discriminating between the traffic that the SOC does need to see and the packets and bytes within that it doesn’t need to see.

The accuracy with which only the right packets are forwarded to the SOC is key to keeping the lid on capex and opex costs.

What’s also important is that a Traffic Policy Engine should be easily customizable because each telco organization’s security requirements – the way different flows and different packets are perceived from a risk perspective – are not only different from one another but are also subject to frequent changes.

Bearing Down on Compute, Network and Storage Costs

When you consider the colossal scale at which this is taking place in the case of even the smallest telcos and ISPs, it becomes clear that hardening security posture against changes in traffic volume and traffic profiles is just one half of the challenge facing telco SOC operations. The other half is doing it in a way that can scale cost effectively. If you’re having to handle 30% - 40% more traffic every year, and you’re also having to do different, innovative, things to mitigate the new types of risk from some of that traffic, there’s a significant risk of costs escalating.

Containing Compute Costs

Bearing down on those costs requires taking into account the impact of any chosen approach on compute, network and storage costs throughout the SOC environment. The previous section detailing policy tools already alluded to the impact on compute resources. Security tools like Intrusion Detection Systems and Intrusion Protection Systems (IDS/IPS) are resource intensive. You only want them being sent packets that they can actually act on. At the same time, you want them to receive as much information about a packet as they need to make a good decision, but no more than that. And you don’t want any instances of a given tool falling over for any reason, especially if there are other instances of that same tool being under-utilized elsewhere in the environment. An approach that falls short on those targets inevitably means that some amount of the investment in security tools is being wasted.

The other way to keep the lid on compute costs is through extreme scalability in traffic inspection, classification and optimization given the CPU workload that’s needed for packet processing. That’s a function of core processing capacity, speed of interfaces supported, form factor and key metrics like capacity per footprint. How many filters can be supported in a telco environment where requirements run into the several tens of thousands of filters (or even several hundred thousand in some cases) is also key.

Containing Storage Costs

Storage is also a key cost consideration. With encrypted flows, the case for storage varies. It can be entirely appropriate for a security team to store those packets for a month or two (or even a year or two). But in the case of payloads that can't be decrypted, it's important to avoid the cost of storing those for no good reason. There's no sense in committing resources to storing something like streaming video either.

Containing Network Costs

On the network side, there are two main factors. The first is the total bandwidth needed to support the traffic that's forwarded from the security monitoring staging post to the SOC. Best in class inspection, classification and optimization can substantially reduce the amount of network capacity needed to backhaul that traffic. Also, where greater distribution of the network architecture is driven by requirements like 5G, the SOC architecture is liable to follow suit. Further efficiencies can then be gained from a solution being able to forward traffic to the optimal location, whether central or distributed.

With encrypted payloads that can't be decrypted, it's important not to incur the cost of storing those for no good reason.

NetQuest's New Network Security Broker

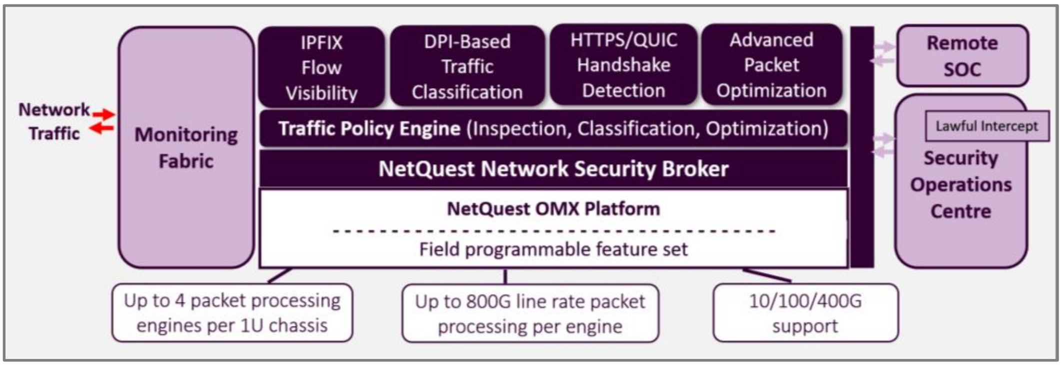
Mount Laurel, New Jersey-based NetQuest Corporation has defined a new category of highly scalable network security product – a Network Security Broker (NSB) – to meet these telco SOC requirements for more granular traffic inspection, classification and optimization with ultra-high scalability. It can be deployed either at peering links or at network gateways such as Broadband Network Gateways (BNGs) in fixed networks or 4G P-Gateways (PGW) and 5G User Plane Functions (UPF) in mobile networks.

Already known for its Streaming Network Sensors (SNS) product for network flow intelligence and WAN Signals Probes (WSP) product for WAN monitoring, the new NSB is the third telco scale network monitoring and network security application running on NetQuest's widely deployed, field programmable OMX platform. As shown in **Figure 4** the OMX is a compact-modular 1U chassis supporting up to four packet processing modules that support 10/100/400 Gig interfaces.

Inspection, Classification and Optimization with Ultra-High Scalability

The NSB's core differentiators are unique traffic inspection, classification and optimization together with ultra-high scalability. Its useful to define the NSB market space at a high level. The best way to do that is relative to the nearest equivalent networking or network security products that are deployed in telco networks today. And if you want to filter and forward only relevant traffic to a telco SOC, the closest, potentially most relevant, product types for doing that before Network Security Brokers have been Network Packet Brokers and Firewalls.

Figure 4: The New Network Security Broker from NetQuest


Network Traffic
Monitoring Fabric
IPFIX Flow Visibility
DPI-Based Traffic Classification
HTTPS/QUIC Handshake Detection
Advanced Packet Optimization
Traffic Policy Engine (Inspection, Classification, Optimization)
NetQuest Network Security Broker
NetQuest OMX Platform
Field programmable feature set
Remote SOC
Lawful Intercept
Security Operations Centre
Up to 4 packet processing engines per 1U chassis
Up to 800G line rate packet processing per engine
10/100/400G support

Source: HardenStance/NetQuest

Higher scalability compared with Network Packet Brokers…

Compared with a Network Packet Broker, a Network Security Broker has two fundamental differentiators:

- **It is a dedicated Traffic Policy Engine**. Most Network Packet Brokers do both packet switching and some traffic optimization. A Network Security Broker is purpose-built for traffic optimization – the monitoring fabric piece is delegated to low cost switching infrastructure augmented with VLAN tagging and load balancing.
- **It supports very much higher scalability**. In part because it is dedicated solely to the Traffic Policy Engine function, but more so because it runs on field programmable hardware, a Network Security Broker is far more scalable than a Network Packet Broker. Network Packet Brokers typically implement traffic optimization functions using network processors which tends to drive the requirement for a lot of racking and stacking in telco environments.

SOC grey listing addresses the majority of traffic in a telco network which is traffic that the SOC only needs to see a small subset of or is only able to see a small subset of.

…and compared with Firewalls too (though for different reasons)

A Network Security Broker has the same high scalability differentiator relative to a Next Generation Firewall (NGFW) – but for different reasons. Although it can potentially be used in-line as well as in stateful mode for some use cases, the Network Security Broker typically operates out of band and filters in stateless mode. As a staging post for identifying and forwarding relevant traffic to the SOC, a Network Security Broker only needs to support coarse-grained filtering; fine-grained inspection is done by security tools in the SOC. This balance of features in a Network Security Broker consumes far less resources than firewalls that are optimized for in-line, stateful, fine-grained filtering. That drives the differentiator in scalability.

Traffic Inspection, Classification and Optimization

NetQuest's Network Security Broker is built on FPGAs and applies policies at line rate. DPI-based filtering is done at truly telco scale. The Network Security Broker is driven by an advanced library function that supports two different types of managed objects. As shown below these are:

- **Telco-scale IP address lists** which are used to tie IP address filters to tunnelling protocols like GTP or GRE at a scale of over 1 million filters per 1U OMX platform. These are applied at either the outer or inner tunnel level. For example, in 5G monitoring they're applied at the outer GTP tunnel level to identify Control Plane traffic between the operator's own service platforms and at the inner level for subscriber traffic.
- **Lists of those services that the SOC wants to see.** Libraries of lists that the SOC team cares about can be built - from basic protocol port-pairs to DPI-based service detections such as HTTPS or HTTP3/QUIC handshake packets.

In conjunction with these telco scale address and service lists, the Network Security Broker provides SOC blacklisting and whitelisting. But in the context of today's requirements, this is no more than basic table stakes for a Traffic Policy Engine. It only addresses the minority of traffic that falls into one or other binary classification of the telco SOC needing to either see all of it or none of it.

SOC Greylisting is a Key Differentiator

A key differentiator of the Network Security Broker is that it also supports SOC greylisting. This addresses the majority of traffic in a telco network which is traffic that the SOC only needs to see a small subset of (like video streams) or is only able to see a small subset of (like encrypted flows). The SOC does typically need to see critical connection establishment and accounting information from these flows. However, most packets within these classes of traffic are of little or no value from a security perspective.

A Solution That Fits a Number of Different Telco SOC Use Cases

No two telecom network architectures are the same. No two telecom operator's traffic profiles are the same. And no two telecom operator's network security policies – developed in conjunction with the unique requirements of their national telecom and national security regulatory agencies - are the same.

For that reason, the use cases for a Network Security Broker – the different architectures in which it is deployed, the different features that a given telecom operator chooses to take advantage of – can be expected to differ quite significantly from one operator to the next, depending on what kind of monitoring infrastructure they have in place.

The following two different use cases are broadly representative of the diversity of requirements:

- Having a relatively advanced, well-engineered, universal monitoring fabric that creates a high level of visibility tends to drive a distributed passive model. Traffic can be peeled off from the production network at the Service Provider Edge for the Network Security Broker to optimize and forward relevant traffic to the SOC.
- Limited visibility or visibility in silos is more likely to drive a model with point deployments of Network Security Brokers to optimize traffic for more targeted security monitoring.

At a summary level, the core suite of the Network Security Broker's inspection, classification and optimization features can be characterized as follows:

1) **DPI-Based Traffic Classification:** A telco SOC can't rely on Port 80 carrying clear traffic and Port 443 carrying encrypted traffic. So the ability to identify and separate out encrypted flows, streaming video and the like is supported.
2) **HTTPS/QUIC Handshake Detection:** applying deep packet inspection, valuable handshake packets can be detected, classified and forwarded to the SOC while optimizing the remaining encrypted packets in the flow.
3) **Traffic Optimization:** examples of the techniques supported are truncating and shunting whereby only a subset of bytes in a packet or only a subset of packets in a flow is forwarded.
4) **1:1 IPFIX Flow visibility:** stateful flow metering is supported to record and track every single flow, packet and byte so the SOC can capture and compare exactly what traffic came into the monitoring environment, exactly what was forwarded on, and the delta between the two.

The increasing volume and evolving nature of network traffic is demanding a smarter approach to maintaining visibility while controlling costs. Launching in Q4 2022, NetQuest's Network Security Broker provides powerful traffic controls for substantially improving the scalability of existing security tools, while reducing a telco SOC's networking and storage costs. ■

About NetQuest Corporation

NetQuest designs, manufactures and markets advanced cyber intelligence solutions to network service providers, large enterprises and government agencies for national defense and network security applications. Founded in 1987 and based in Mount Laurel, New Jersey, NetQuest is an employee-owned business. With a proven track record of providing cutting edge cyber solutions, NetQuest has developed a global customer base, marketing directly and through a network of strategic partners, value-added resellers and representatives. For more information, visit https://www.netquestcorp.com.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, MEF OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.